The Intel® IXP2850 An Enhanced 10 Gbps Network Processor With Integrated Security Accelerator

Microprocessor Forum, October 15, 2002

(Note: Intel® Confidential, Embargoed prior to 10/15/02)

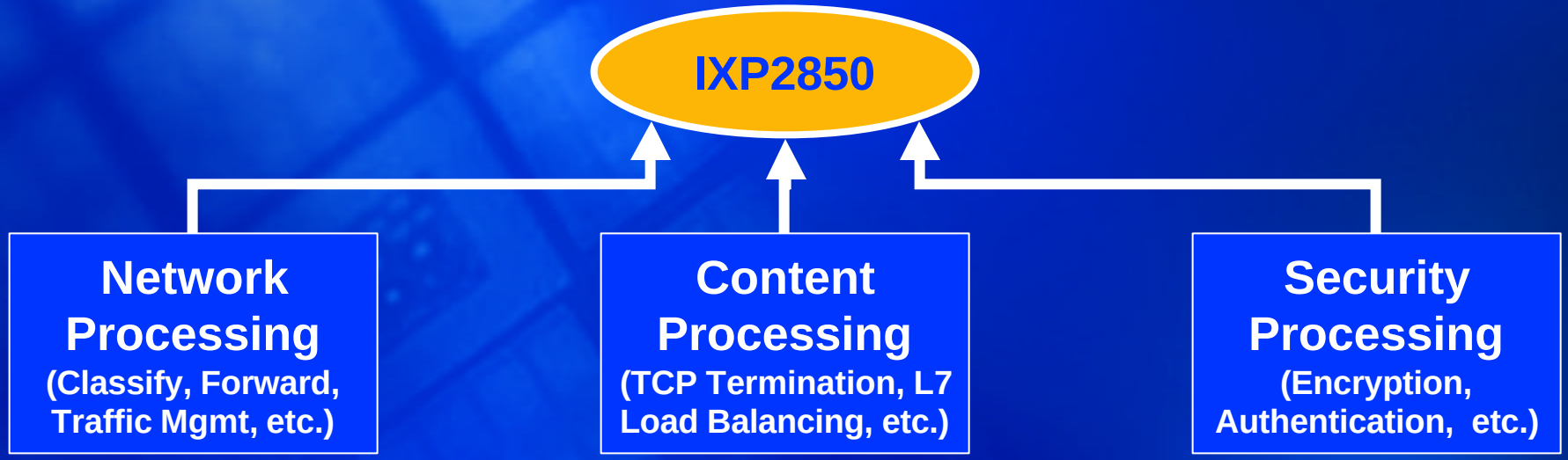
Matthew Adiletta
Intel® Fellow
Director of Communications Processor Architecture
Intel Corporation

intel

Agenda

- Introduction
- Secure Content Processing Requirements
  - Benefits of Crypto & NPU Integration
- Intel® IXP2850 Network Processor Device Architecture
- Typical Crypto Data-Flow
- Crypto Unit Overview & Algorithm Details
- Performance Characteristics
- Software & Hardware Partitioning
- Example Software Details
- Summary

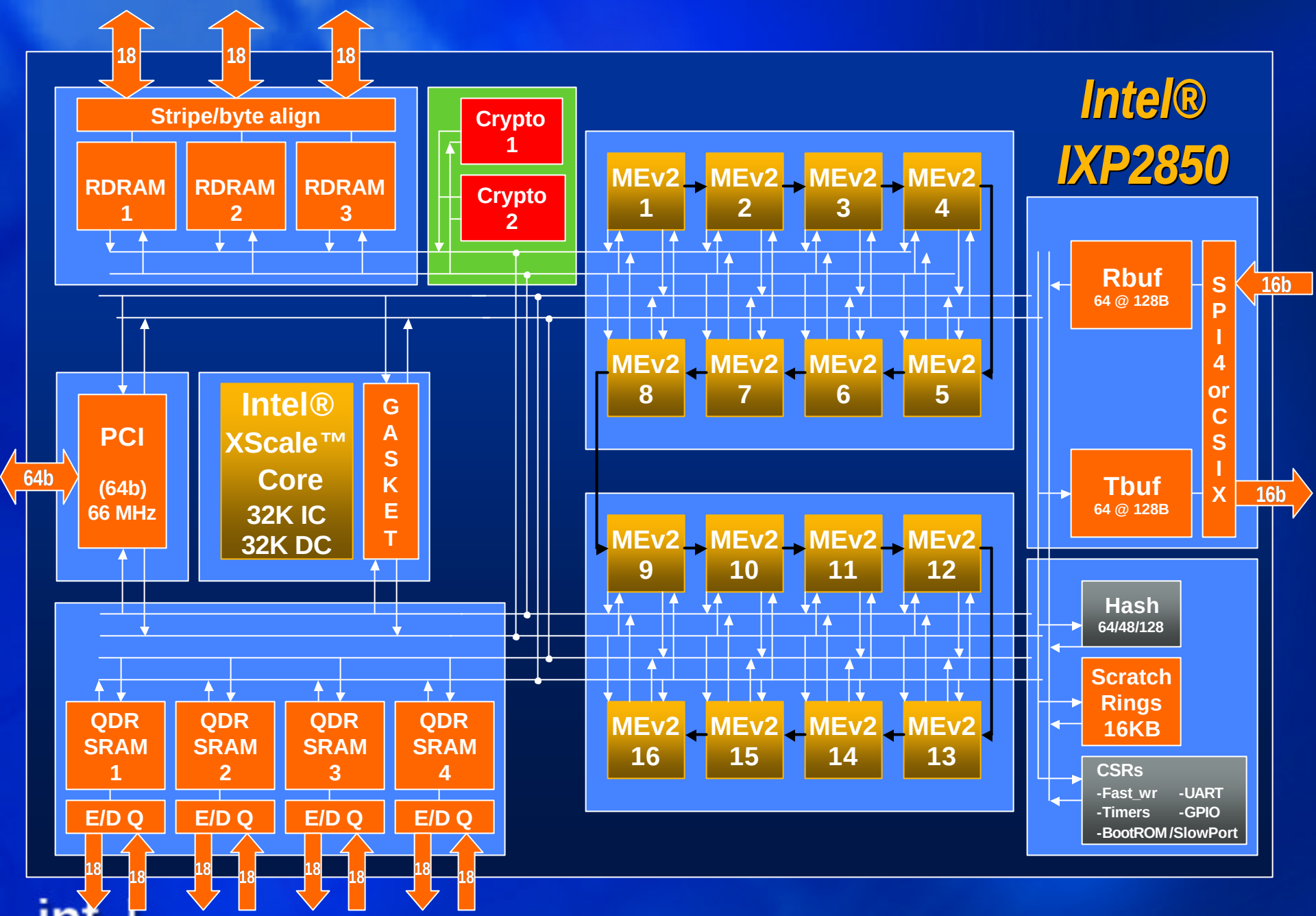
A Platform for Secure Content Processing



- The Intel® IXP2850 integrates a 10Gbps Cryptographic Processor and a 10 Gbps Network Processor to enable secure content processing applications
- Modular protocol termination & content processing software enables rapid TTM for rich applications
- High performance & integration deliver reduced cost, power consumption & real-estate at the line card level

Value Proposition - NPU & Security Integration?

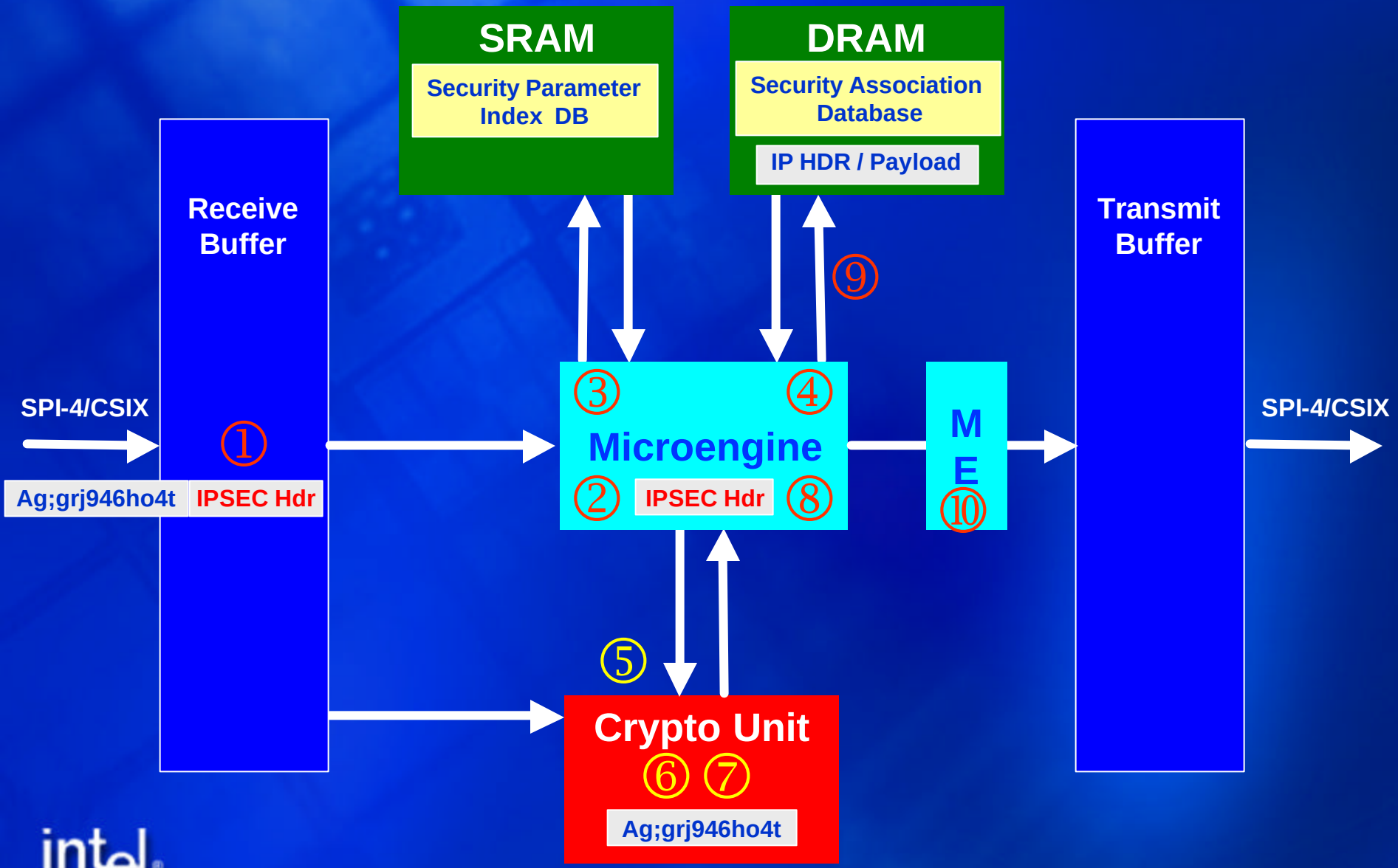
- Security Algorithms are “Hard” (hardware acceleration)
  - Delivers high performance with power, silicon area, cost & PCB board real estate savings
- Protocols are “Soft” (Microcode & Intel® Xscale™ Software)
  - Protocol software can be optimized for different system environments (IPSEC/SSL/etc.)
  - Protocol termination / translation is a native function of the NPU
    - Can support new protocols such as IPv6, SCTP, etc.
  - Programmers can optimize TCP / IPSEC for different applications
    - Many sessions/second, SSL
    - High throughput, iSCSI
- Tightly coupled NPU & Crypto allows optimized used of memory
  - Security Policy and classification operations can be combined
  - Common data structures (e.g. Security Association Database) offer zero copy access - minimizing bus traffic and simplifying management software



intel

Pin and Software Compatible with Intel® IXP2800

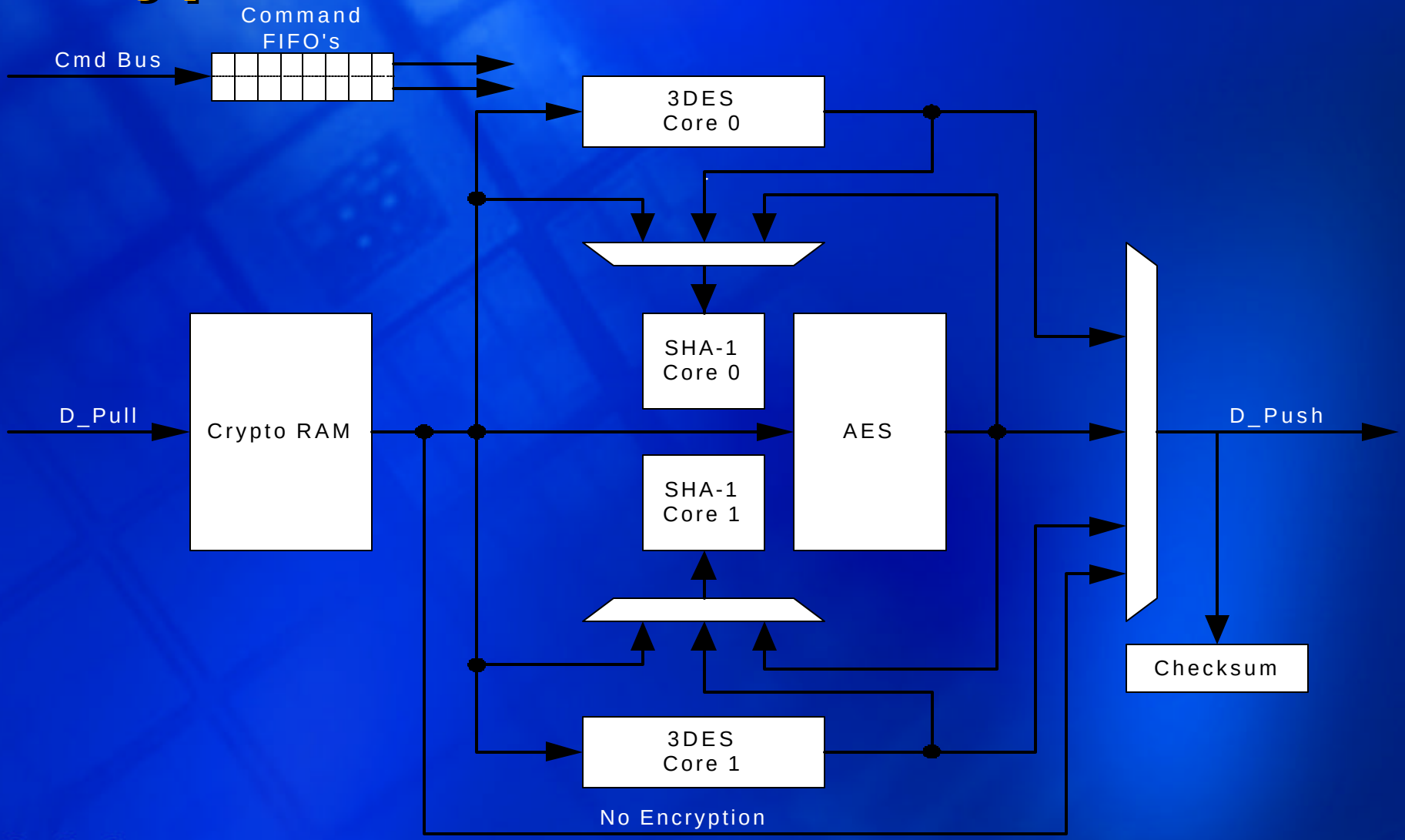
A Typical IPSEC Data Flow



Crypto Unit Features

- Intel® IXP2850 integrates 2 independent crypto units
  - Multiple independent algorithm engines in each unit
    - DES/3DES, AES, SHA-1
  - Aggregate throughput supports 10Gb line rates
- Flow-through architecture supports 10Gb rates
  - Packet does not need reassembly – crypto operations are performed on “chunks” of the packet on the fly
- Internal state management allows efficient packet interleaving at high rates
  - New state can be pre-loaded in the background while cores are running
- Hardware Checksum offload after encryption for TCP

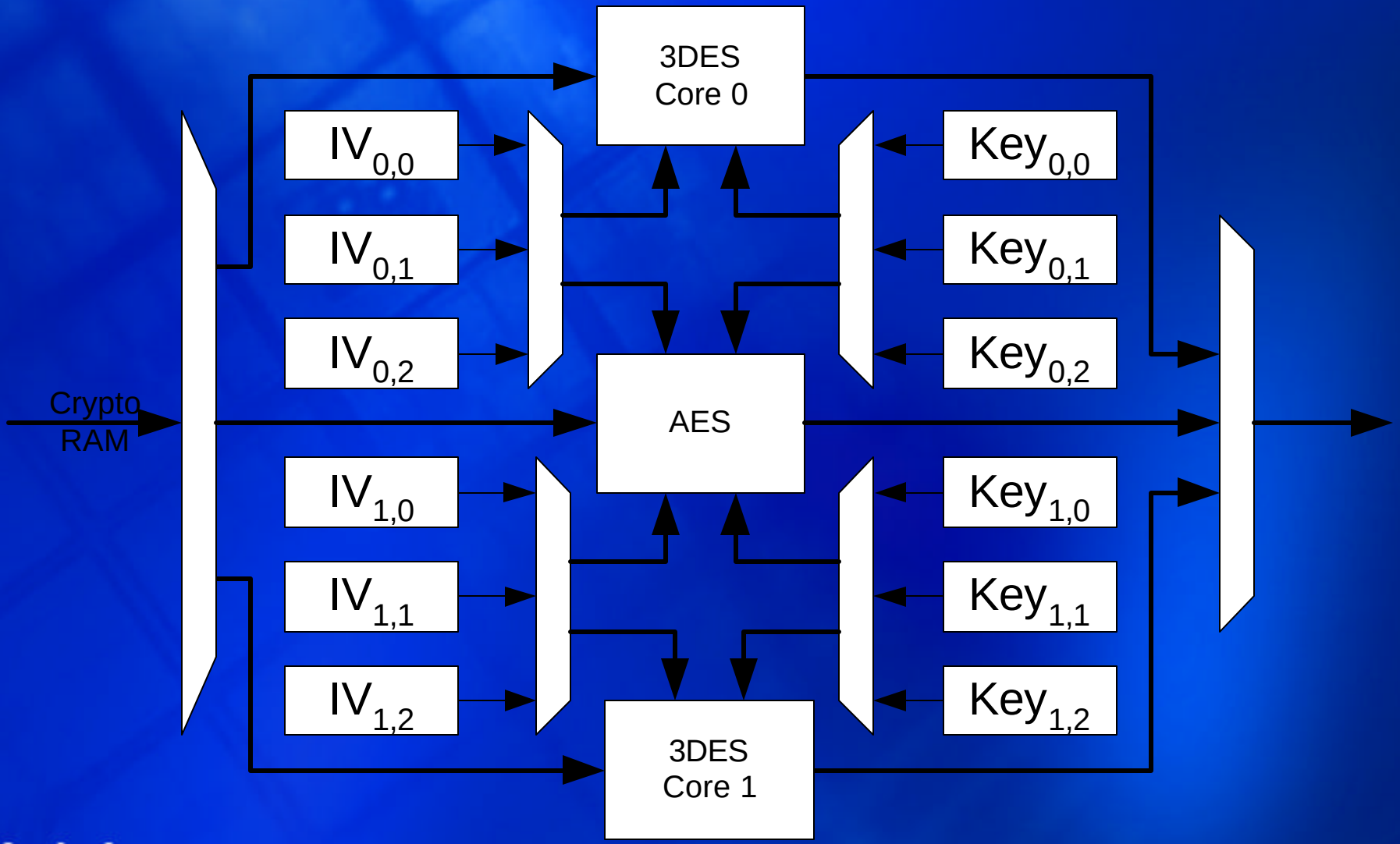
Crypto Unit Overview



Symmetric Crypto Algorithms

- AES
  - All key sizes, CBC and direct access
- 3DES
  - Support for DES, CBC and direct access
- SHA-1
  - HMAC support
  - Before or after cipher
- MD5, RC4
  - Supported via microcode implementation in ME's

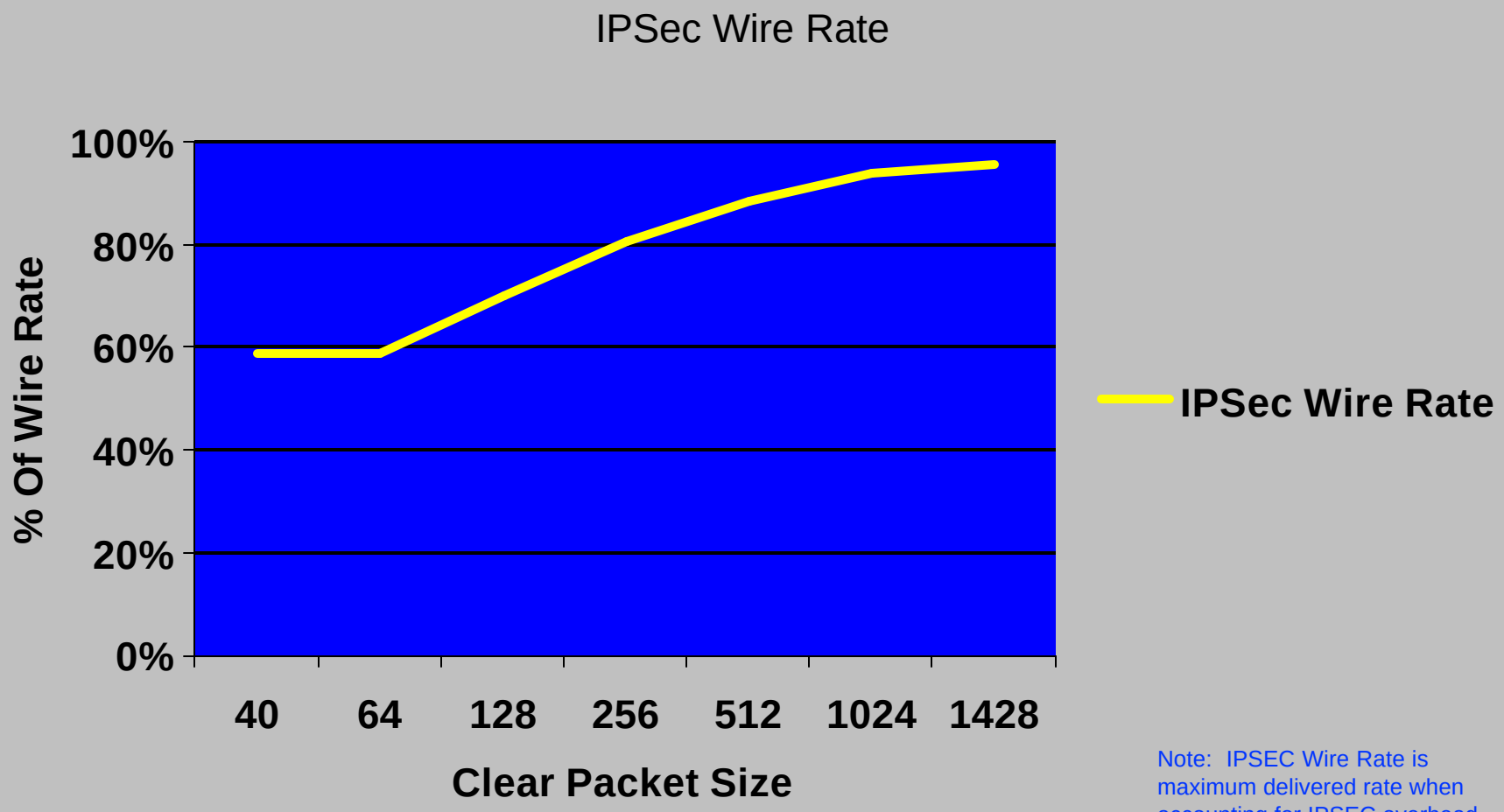
Cipher Data Path



Core Algorithm Performance

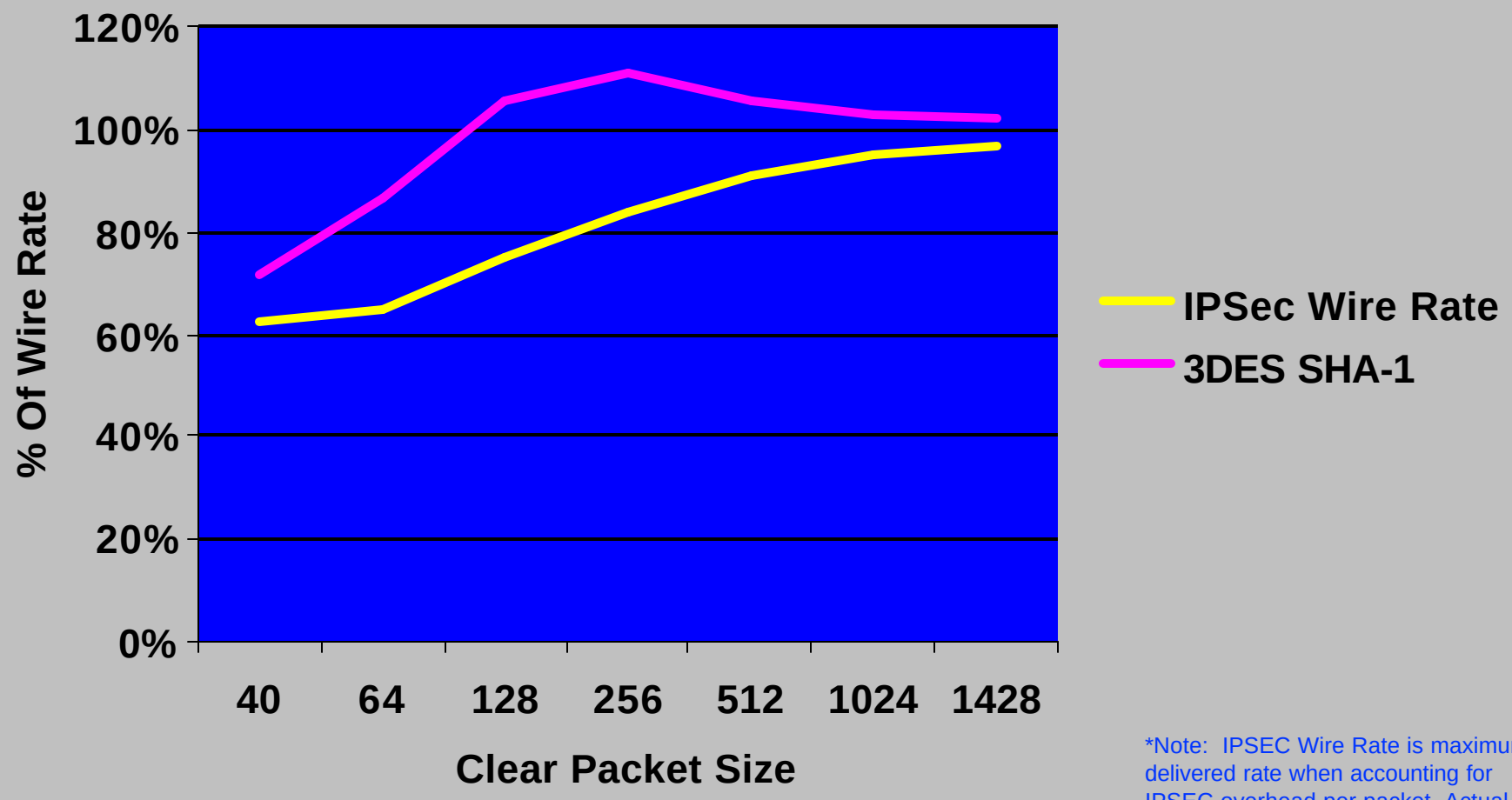
	Cycles		Mbit/Second	
	Block	64 Bytes	1 Core	Total
SHA-1	88	88	4,073	16,291
3DES	18	144	2,489	9,956
AES-128	21	84	4,267	8,533
AES-192	25	100	3,584	7,168
AES-256	29	116	3,090	6,179

Achievable IPSec Wire Rate



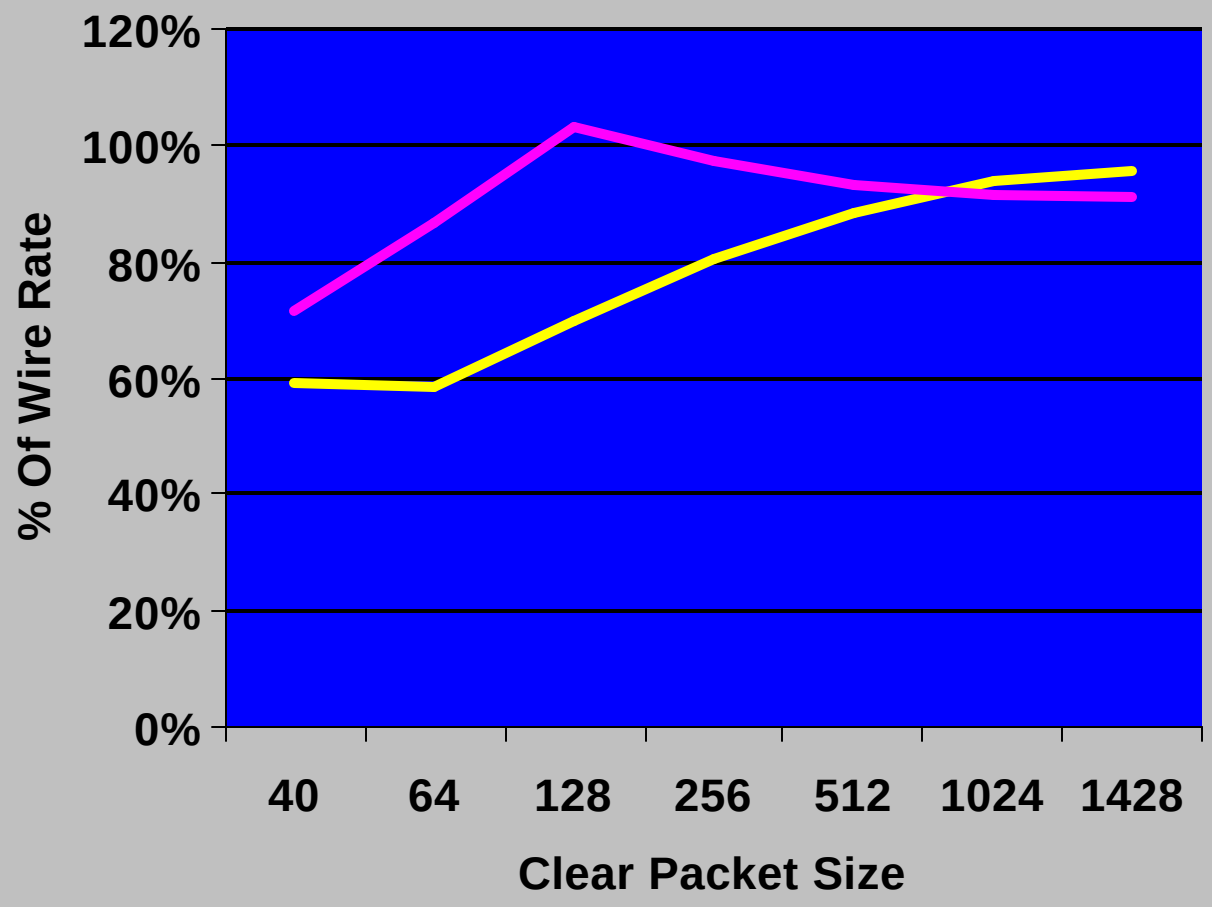
Note: IPSEC Wire Rate is maximum delivered rate when accounting for IPSEC overhead per packet

Intel® IXP2850 ESP 3DES SHA-1 Performance Estimates*



*Note: IPSEC Wire Rate is maximum delivered rate when accounting for IPSEC overhead per packet. Actual performance in system may vary.

Intel® IXP2850 ESP AES-128 SHA-1 Performance Estimates*



*Note: IPSEC Wire Rate is maximum delivered rate when accounting for IPSEC overhead per packet. Actual performance in system may vary.

IXP Crypto Software Architecture

Basic Software Partitioning

- High Layer Protocols (XScale™)

iSCSI	IKE	SSL	TLS	WTLS

- Fast Path Protocol Acceleration
  (Microengines & Intel® XScale™)

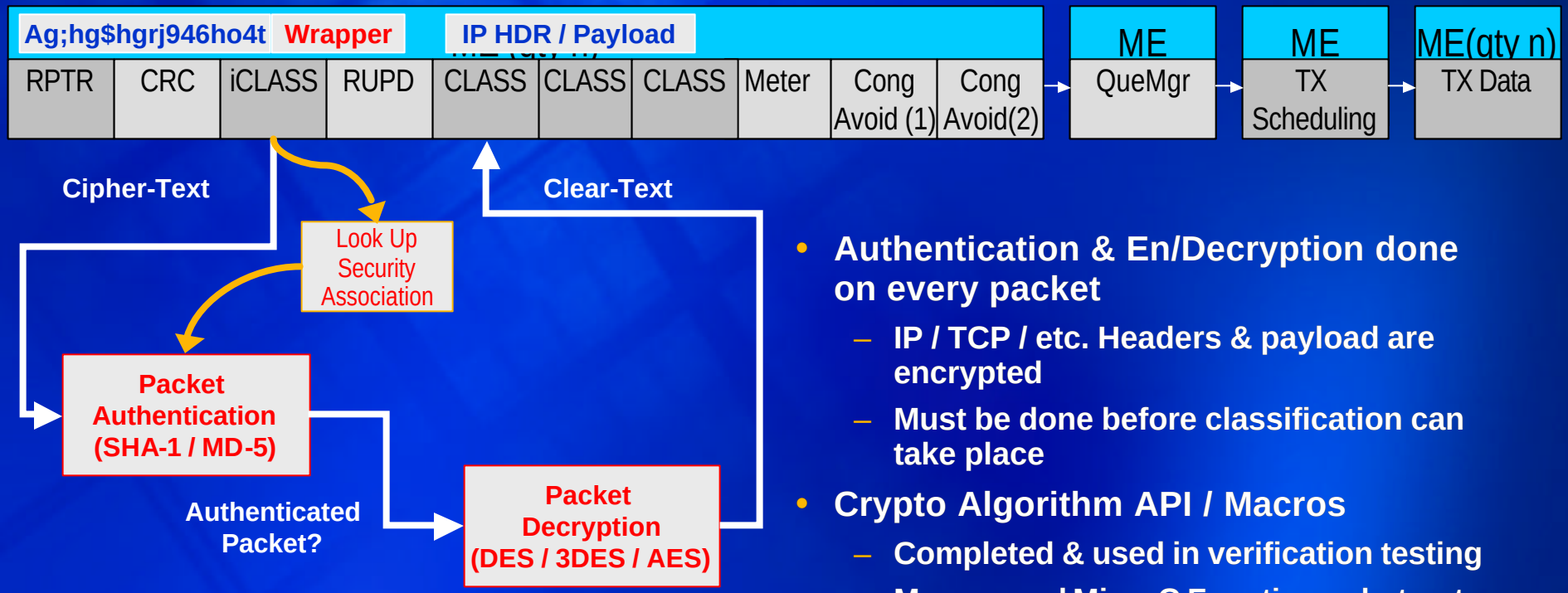
TCP	SCTP	UDP	IPSEC

- Algorithms (H/W Acceleration)

3DES	DES	AES	SHA-1	MD-5 (uCode)	RC4 (uCode)

Fast Path Software
- Where does Crypto come in?

IPSEC Ingress Pipeline Partitioning:



- **Authentication & En/Decryption done on every packet**
  - **IP / TCP / etc. Headers & payload are encrypted**
  - **Must be done before classification can take place**
- **Crypto Algorithm API / Macros**
  - **Completed & used in verification testing**
  - **Macros and MicroC Functions abstract crypto functions**

Key Messages

- Intel® IXP2850 extends the Intel® IXP2000 family NPU performance with best-in-class security acceleration on-chip
  - The highest performance commercial crypto engine*
  - Pin & Software Compatible upgrade from Intel® IXP2800
- NPU & Crypto Integration helps remove cost, power and real-estate barriers to deploying security apps

- External Features
  - Enhanced SPI-4.2 Media / Switch Fabric Interface
  - 3 X 16-bit RDRAM Channels (50+ Gbps raw bandwidth)
  - 3 x 250 MHz QDR / SigmaRAM SRAM Channels
  - 64-bit / 66 MHz PCI Interface
- Internal Features
  - 16 x 1.4 GHz 32-bit Microengines
  - 700 MHz Intel® XScale™ Control Plane Processor
  - 10 Gbps Security Accelerator
  - 50M+ Transistors, 0.13 Micron Process

Source: Intel® estimates & The Linley Group – A Guide to Security Processors